RECEIVED
CENTRAL FAX CENTER
OCT 17 2008

Amendments to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (Currently Amended) A method of authenticating candidate members wishing to participate in an IP multicast via a communication network, where data sent as part of the multicast is to be secured using a key revocation based scheme ~~requiring that each candidate member submit a public key to a group controller in order to become a participating candidate member,~~ the method comprising:

a candidate member receiving an invitation from a group controller to join the multicast;

the candidate member sending a registration message to the group controller, the registration message including the candidate member's originating IPv6 address, a copy of the candidate member's public key from the candidate member's public-private key pair and a digital signature using the candidate member's private key from the candidate member's public-private key pair;

at the group controller, verifying that the public key received from ~~each~~ the candidate member wishing to participate is owned by the ~~that~~ candidate member and that the public key is associated with the respective candidate member's IPv6 [[IP]] address ~~of that candidate member~~ by inspecting an interfaceID part of the IPv6 [[IP]]address; and.

using the digital signature, further verifying that the candidate member owns the public-private key pair to which the public key belongs and that the candidate terminal owns the source IP address.

2. (Currently Amended) [[A]] The method according to claim 1, wherein said key revocation based scheme is a Logical Key Hierarchy based scheme.

3. (Currently Amended) [[A]] The method according to claim 1, wherein each candidate member generates [[an]] the interfaceID part of the candidate member's IPv6 ~~its own IPv6~~ address by taking a cryptographic hash over the candidate member's own public key and one or more other parameters~~, and the candidate member sends a joining request to the group controller which contains:~~

~~the member's IPv6 [[IP]] address including the generated interface ID;~~

~~the candidate member's own public key; and~~

~~a signature over the entire message generated using the member's private key~~.

4. (Currently Amended) [[A]] The method according to claim 3, wherein upon receipt of the message, the group controller:

a) ~~uses~~ using the received public key to confirm that the signature is valid, thus proving that the candidate member does indeed own the public-private key pair to which the received public key belongs and

b) ~~applies~~ applying the same cryptographic hash, as used by the candidate member, to the public key and the other parameter (s) and comparing ~~compares~~ the result to the interfaceID part of the candidate member's IPv6 [[IP]] address, thus verifying that the source IPv6 [[IP]] address is owned by the candidate.

5. (Currently Amended) [[A]] The method according to claim 2, wherein, after the group controller has received the public key from a given candidate member and has verified that the public key is associated with the IPv6 [[IP]] address of the sender, the group controller sends a unique Key Encryption Key to the member, encrypted with that member's public key, and the group controller also sends a Traffic Encryption Key and a LKH key set to the member, encrypted with the Key Encryption Key.

6. (Currently Amended) [[A]] The method according to claim 1, wherein said IP multicast comprises:

a one-way multicast where a single node multicasts a stream of data to several other nodes;

a group multicast where group members multicast data to all other members of the group; or

a tele-conference or a videoconference or a multimedia conference.

7. (Currently Amended) A method of authorizing ~~authorising a~~ user to participate in a secure IP multicast or broadcast ~~in which security keys are distributed to group members using a key revocation based mechanism~~, the method comprising:

distributing security keys to users using a key revocation based mechanism;

delivering a certificate to the user, the certificate verifying that a public-private key pair identified in the certificate can be validly used by the user to access said secure multicast/broadcast, wherein the certificate further includes a digital signature generated by applying an algorithm and the user's private key to the contents of the certificate;

subsequently verifying at a control node that the certificate is owned by the user using a proof-of-possession procedure that is based on the private key; and

assuming that verification is obtained, using said public key to send a Key Encryption Key to the user.

8. (Currently Amended) [[A]] The method according to claim 7, wherein said key revocation based scheme is a Logical Key Hierarchy based scheme.

9. (Currently Amended) [[A]] The method according to claim 8, wherein said step of verifying at [[a]] the control node that the certificate is owned by the user, is carried out after the control node receives a request from the user to join said secure multicast or broadcast.

10. (Currently Amended) [[A]] The method according to claim 7, wherein said proof-of-possession procedure involves the control node sending a random number to the user in plain text, and the user sending a response to the control node containing

a signature generated by applying the private key to the random number, wherein the control node is in possession of the user's certificate and can check whether or not the message is correctly signed with the user's private key.

11. (Currently Amended) [[A]] The method according to claim 7, wherein the user to be authorized ~~authorised~~ has a subscription to a first, home communication network and wishes to participate in a multicast or broadcast service via a second, visited ~~foreign~~ network in which the user is roaming, the method comprising:

the visited network, in which the user is roaming, contacting the user's home network, upon receipt of an initial registration request from said user, to authorize ~~authorise~~ the user;

following authorization ~~authorisation~~ by the home network, generating a certificate relating to said service and generating [[a]] the public-private key pair, either at the user equipment or within one of the networks, and signing the certificate; and

sending the certificate to the user.

12. (Currently Amended) [[A]] The method according to claim 11, wherein an Authentication and Key Agreement (AKA) procedure is used to authorise the user.

13. (Currently Amended) A group controller for authenticating candidate members wishing to participate in an IP multicast via a communication network, where data sent as part of the multicast is to be secured using a key revocation based scheme requiring that each candidate member submit a public key to the [[a]] group controller in order to become a participating candidate member, the group controller comprising:

means for sending an invitation to a candidate member to join the multicast;

means for receiving from the candidate member a registration message, the registration message including the candidate member's originating IPv6 address, a copy of the candidate member's public key from the candidate member's public-private key

pair and a digital signature using the candidate member's private key from the candidate member's public-private key pair;

means for verifying that the public key received from the ~~each~~ candidate member wishing to participate is owned by the ~~that~~ candidate member and that the public key is associated with the ~~IP address of that~~ candidate member's IPv6 address by inspecting an InterfaceID part of the IP address

means for using the digital signature for verifying that the candidate member owns the public-private key pair to which the public key belongs and that the candidate terminal owns the source IP address.

14. (Canceled)

15. (Currently Amended) [[A]] The group controller according to claim 13, wherein said key revocation based scheme is a Logical Key Hierarchy based scheme.

16. (Currently Amended) [[A]] The group controller according to claim 13, further comprising:

means for receiving and storing a generated interfaceID part of a candidate member's ownIPv6 address and for receiving a joining request from the candidate member to the group controller which contains:

the member's IPv6 [[IP]] address including the generated interface ID;

the candidate member's own public key; and

a signature over the entire message generated using the member's private key.

17. (Currently Amended) [[A]] The group controller according to claim 16, further comprising means for, upon receipt of the message:

using the received public key to confirm that the signature is valid, thus proving that the candidate member does indeed own the public-private key pair to which the received public key belongs; and

applying a ~~the same~~ cryptographic hash, used by the candidate member, to the public key and other parameters and ~~compare~~ comparing the result to the interfaceID part of the candidate member's IPv6 [[IP]] address, thus verifying that the ~~source~~ IPv6 [[IP]] address is owned by the candidate member.

18. (Currently Amended) [[A]] The group controller according to claim 17, wherein, after the group controller has received the public key from a given candidate member and has verified that the public key is associated with the IP address of the sender, the group controller having:

means for sending a unique Key Encryption Key to the candidate member, encrypted with that candidate member's public key; and

means for sending a Traffic Encryption Key and a LKH key set to the candidate member, encrypted with the Key Encryption Key.

19. (Currently Amended) [[A]] The group controller according to claim 13, wherein said IP multicast comprises:

means for a single node multicasting a stream of data to several other nodes;

means for a group multicast where group members multicast data to all other members of the group; or

means for a tele-conference or a videoconference or a multimedia conference.

20. (Currently Amended) A group controller for authorizing ~~authorising~~ a user to participate in a secure IP multicast or broadcast ~~in which security keys are distributed to group members using a key revocation based mechanism~~, the group controller comprising:

means for distributing security keys to the user using a key revocation based mechanism;

means for delivering a certificate to the user, the certificate verifying that a public-private key pair identified in the certificate can be validly used by the user to access said secure ~~multicast/broadcast~~ multicast or broadcast, wherein the certificate includes a digital signature generated by applying an algorithm and the user's private key to the contents of the certificate;

means for subsequently verifying at a control node that the certificate is owned by the user using a proof-of-possession procedure that is based on the private key; and

means for assuming that verification is obtained, using said public key to send a Key Encryption Key to the user.

21. (Currently Amended) [[A]] The group controller according to claim 20, wherein said key revocation based scheme is a Logical Key Hierarchy based scheme.

22. (Currently Amended) [[A]] The group controller according to claim 21, wherein means for verifying at [[a]] the control node that the certificate is owned by the user, also verifies the certificate after the control node receives a request from the user to join said secure multicast or broadcast.

23. (Currently Amended) [[A]] The group controller according to claim 20, wherein the control node further comprises:

means for sending a random number in a message to the user in plain text; and

means for receiving from the user a response containing a signature generated by applying the private portion of the public-private key to the random number, wherein the control node is in possession of the user's certificate and can check whether or not the message is correctly signed with the user's private key.

24. (Currently Amended) [[A]] The group controller according to claim 20, wherein the user to be authorized ~~authorised~~ has a subscription to a first, home communication network and wishes to participate in a multicast or broadcast service via

a second, visited ~~foreign~~ network in which the user is roaming, the group controller including means for:

the visited network, in which the user is roaming, contacting the user's home network, upon receipt of an initial registration request from said user, to authorize ~~authorise~~ the user

receiving from the visited network contacting the user's home network, upon receipt of an initial registration request from said user, to authorize ~~authorise~~ the user;

means for generating [[a]] the certificate relating to said service following authorization ~~authorisation~~ by the home network;

means for generating [[a]] the public-private key pair and signing the certificate; and

means for sending the certificate to the user.

25. (Currently Amended) [[A]] The group controller according to claim 20, wherein an Authentication and Key Agreement (AKA) procedure is used to authorize ~~authorise~~ the user.